UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

UNITED STATES OF AMERICA,)
)
Plaintiff,)
)
v.) Case No. 4:16-CR-00258-HEA-NAB-1
)
ALDEN DICKERMAN,)
)
Defendant.)

REPORT AND RECOMMENDATION OF MAGISTRATE JUDGE

The above matter was referred to the undersigned United States Magistrate Judge pursuant to 28 U.S.C. § 636(b). This matter came before the undersigned for an evidentiary hearing on April 19, 2017 on the First Motion to Suppress Evidence and Statements [Doc. #20]; First Motion for *Franks* Hearing [Doc. #21]; and Defendant's Supplemental Motion to Suppress Evidence [Doc. #33]. At the hearing, The United States of America "the Government" was represented by Assistant United States Attorneys Colleen Lang and Robert Livergood, Defendant Alden Dickerman was represented by Adam Fein. Following the hearing, a transcript was prepared and the parties completed filing post-hearing memoranda on August 2, 2017.

Defendant was charged by indictment with possession of child pornography in violation of 18 U.S.C. §2252A(a)(5)(B) after law enforcement officers executed a search warrant at his residence and seized evidence from a laptop computer and hard drive found inside the home. Defendant seeks suppression of evidence derived from the search and of statements Defendant made at the time of the search. Defendant argues that the warrant was not supported by probable cause; that the searches and seizures of data and electronic communications through law enforcement's use of the Freenet software violated Defendant's Constitutional privacy rights;

and that all contents including pictures and videos found after search of Defendant's laptop were poisonous fruit of the unlawful search and seizure of the laptop. Defendant also filed a Motion for a *Franks* hearing alleging that the affidavit in support of the search warrant was inherently misleading and contained false statements and relevant omissions.

In its initial Response to Defendant's Motion to Suppress [Doc. #27], the Government states that the affidavit in support of the search warrant was supported by ample probable cause and did not contain false statements. The search warrant was executed properly and the evidence was properly searched. In its Response to Defendant's Motion for Franks Hearing [Doc. #28]], the Government states that Defendant failed to identify any statements in the affidavit that were deliberately or recklessly false. The Government also states that any omitted truthful statements have not been shown to affect the probable cause determination. In its Response to Defendant's Supplemental Motion to Suppress Evidence and Statements [Doc. #37], the Government argues that law enforcement's collection of basic data on the open source peer-to-peer file sharing program Freenet is not an illegal search or seizure. The Government also contends that the information collected by law enforcement is not an interception of content information nor is it private communications.

I. Facts

At the evidentiary hearing four witnesses testified: St. Louis County Detective Michael Slaughter; Special Investigator Wayne Becker; Professor Brian Levine; and Judge John Borbonus. An affidavit was submitted from Stephen Dougherty. From the testimony and exhibits admitted at the hearing, the undersigned makes the following factual findings.

On August 18, 2015, St. Louis County Detective Michael Slaughter applied for and received a search warrant from St. Louis County Associate Circuit Judge John Borbonus. The warrant authorized the search of 9524 Corregidor Drive in St. Louis, Missouri for evidence of child pornography. [Gov. Exh. 3]. The affidavit in support of the application relies on Special Investigator (SI) Wayne Becker's undercover investigation using the law enforcement version of Freenet beginning in September 2011. *Id.* at 6. Of relevance, the affidavit states that,

> While reviewing requests received by undercover Freenet nodes, located in Missouri, SI Becker observed IP address 172.12.235.62 routing and/or requesting suspected child pornography blocks. *The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requestor of the file*." *Id.* at 7. The affidavit further states that on April 2, 2015, SI Becker observed a computer running Freenet at that IP address request from Freenet law enforcement nodes 69 blocks of a video file (SHA1:BODS262HHKS3VS4FLQSOAAVAWT OE5FAW; File Name: Another Set 2 (set 2).zip) which SI Becker had downloaded and knew to contain child pornography. *Id.* The affidavit goes on to describe, based on Detective Slaughter's training and experience, how Freenet functions, that the software has "attracted persons who wish to collect and/or share child pornography files" and "is not a significant source of music, adult pornography, theatrical movies or other copyright material," and that "streams of requests for blocks of a particular file from an IP address can be evaluated to determine if the IP address is the likely requester of the file.

Id. at 8-9.

Defendant was the only person home during the execution of the search warrant. Defendant admitted to having used Freenet before invoking his *Miranda* rights. Computers were seized from the home and SI Becker determined that Defendant's Asus laptop contained Freenet software and files of child pornography.

A. Overview of Freenet

The following is a description of Freenet as described by its developers in an abstract titled *Freenet: A Distributed Anonymous Information Storage and Retrieval System*.

> Freenet is implemented as an adaptive peer-to-peer network[1] of nodes[2] that query one another to store and retrieve data files, which are named by location-independent keys. Each node maintains its own local datastore which it makes available to the network for reading and writing, as well as a dynamic routing table containing addresses of other nodes and the keys that they are thought to hold. It is intended that most users of the system will run nodes, both to provide security guarantees against inadvertently using a hostile foreign node and to increase the storage capacity available to the network as a whole.
>
> The basic model is that requests for keys are passed along from node to node through a chain of proxy requests in which each node makes a local decision about where to send the request next, in the style of IP (Internet Protocol) routing. Depending on the key requested, routes will vary. The routing algorithms for storing and retrieving data are designed to adaptively adjust routes over time to provide efficient performance while using only local, rather than global, knowledge. This is necessary since nodes only have knowledge of their immediate upstream and downstream neighbors in the proxy chain, to maintain privacy.
>
> Each request is given a hops-to-live limit, which is decremented at each node to prevent infinite chains. Each request is also assigned a pseudo-unique random identifier, so that nodes can prevent loops by rejecting requests they have seen before. When this happens, the immediately preceding node simply chooses a different node to forward to. This process continues until the request is either satisfied or exceeds its hops-to-live limit. Then the success or failure result is passed back up the chain to the sending node. No node is privileged over any other node, so no hierarchy or central point of failure exists. Joining the network is simply a matter of first discovering the address of one or more existing nodes through out-of-band means, then starting to send messages.

[1] Peer-to-peer file sharing is a popular means of obtaining and sharing files free of charge directly from other computer users who are connected to the Internet and who are also using peer-to-peer file sharing software. Peer-to-peer file sharing software is publicly available for download free of charge from the Internet and operates on a particular network which dictates to some extent how the file sharing will occur. *United States v. Thomas*, No. 5:12-CR-37, 2013 WL 6000484, at *2 (D. Vt. Nov. 8, 2013), *aff'd*, 788 F.3d 345 (2d Cir. 2015).

[2] A node is a computer that is running the Freenet program.

Ian Clarke, et al., *Freenet: A Distributed Anonymous Information Storage and Retrieval System, (2000)*, https://www.cs.cornell.edu/people/egs/615/freenet.pdf. (last visited September 22, 2017).

B. Law Enforcement Use of Freenet

Law enforcement maintains multiple nodes on Freenet. Law enforcement has created an algorithm that allows it to log the IP address, key, and date and time of requests that were sent to law enforcement Freenet nodes. (Def. Ex. A at 6.) Law enforcement can then compare these keys to keys of known child pornography. *Id.*

The manifest keys (the table of contents and access key to the table of contents) for much of the child pornography on Freenet are publically available. (Gov't Ex. 1 at 3.) Therefore, using the manifest key, law enforcement can request a suspected child pornography file, verify that it is in fact child pornography, and obtain the block keys for that file. *Id*. With the block keys, law enforcement can log block requests for the file received by its node. *Id*. These "observations" include: the IP address of the peer; the Freenet "location" of the peer; the block, identified by the SHA256 hash value; Hops to Live (HTL); time stamp; an identifier that uniquely identifies the law enforcement node connected to the peer; the number of peers the observed peer reports itself to have; and "other information that is visible to any of the node's peers." *Id.*

Law enforcement then plugs those observations into a specially developed algorithm to determine the original requestor. *Id.* at 4. The algorithm relies on two features of Freenet: (1) that block requests can be mapped back to manifest keys and inserted files and (2) that eliminating requests with an HTL of 16 or below significantly narrows the pool of potential original requestors. *Id*. "[T]he algorithm works by looking at the cumulative number of requests for blocks corresponding to a distinct file of interest made by any single node. It then calculates whether the number of requests observed is most likely what we would expect to observe if the peer were the originator of the requests, or just relaying requests on behalf of other nodes." *Id.*[11] It has a 1.35% false positive rate. *Id.* at 8. The Government states that the algorithm was still being refined at the time of SI Becker's investigation but that he was using a fundamentally similar method.

The law enforcement version of Freenet "executes this logging for use by law enforcement and makes no other changes to the Freenet software." *Id.* at 4. "The algorithm's need for these observations does not require law enforcement to run a version of the Freenet application that modifies, circumvents, or exploits the Freenet protocol. The [law enforcement] node does not target specific nodes, and the standard Freenet software is used without modification for selecting peers. The algorithm requires only that a [law enforcement]-operated Freenet node log requests received from its peers in the normal operation of the Freenet system, and the logged requests are not otherwise actively solicited by the [law enforcement] Freenet node." *Id.* "[T]he [law enforcement]-operated Freenet nodes log requests they would also receive using an unmodified Freenet node, sends no extra information or messages, and exploits none of the information actively on the network." *Id.*

C. Detective Michael Slaughter

Detective Slaughter has worked with the St. Louis County Police Department for more than 12 years. He currently works with the Special Investigations Unit and is a Task Force Officer with the FBI's Exploited Children's Unit. He has worked on crimes involving the exploitation of children for seven years. In that time, he has drafted more than one hundred search warrants looking for child pornography. Detective Slaughter has also been trained on

[11] For the algorithm itself, consult Gov't Ex. 1.

peer-to-peer networks and child pornography. He began the investigation into Defendant Dickerman in 2015. Sergeant Adam Kavanaugh gave him a spreadsheet with information involving an IP address of a computer that had requested a file of child pornography on Freenet. Based on his knowledge of Freenet, he drafted a search warrant for the home associated with the IP address. He presented the warrant to a St. Louis County prosecutor before taking it to Judge John Borbonus. This was not the first warrant regarding peer-to-peer software that he had taken before Judge Borbonus.

D. Judge John Borbonus

Judge Borbonus testified that he received the search warrant application from Detective Slaughter on August 18, 2015. He had reviewed 15-20 applications for search warrants involving peer-to-peer software before he signed the warrant involving Defendant Dickerman's home. The Judge reviewed the entire affidavit before signing the search warrant. Judge Borbonus agreed in cross examination that the affidavit described how the Freenet peer-to-peer network operates. When asked by defense counsel, he could not recall the meaning of some of the terms used in the affidavit. However, upon review of the affidavit, it was clear that all of the terms had been defined.

E. Special Investigator Wayne Becker

SI Becker has worked as a Deputy with the Dent County Sheriff's Department since 2004, has more than 600 hours of police training, and has more than 450 additional hours of training in the investigation of computer use in the exploitation of children, and in the methods of forensic analysis of computers used in criminal activity, including the use of peer-to-peer and file sharing networks. (Def. Ex. A at 6.) SI Becker has an Associate's of Science degree in Data Processing from St. Louis Community College, is a certified forensic examiner, has over 30 years of experience in the Information Technology industry, is an instructor in Basic Electronic Evidence Recovery for the Missouri Internet Crimes Against Children (ICAC) Task Force, and is the Dent County Sheriff's Department's representative to the Missouri ICAC Task Force and coordinates the South Central Missouri Computer Crime Task Force. *Id*.

In his testimony, Becker described Freenet as a peer-to-peer overlay network that uses the internet for communicating between computers running the same Freenet software. On Freenet, various types of files can be exchanged, including video files, image files and documents. Becker then described the process of file sharing on Freenet. When a file is uploaded into Freenet, it gets broken into "blocks." Those blocks are held by multiple users who don't know they have pieces of the file. A top level block has the "table of contents" for the file, called a manifest and there is a key to that manifest. The key to a file is a SHA256 hash of the little block of file and those are contained within the high-level manifest block. The "manifest key" is what is shared to retrieve the file. The manifest keys are generally found on free sites or message boards where people exchange keys to files.

SI Becker and other investigators began investigating Freenet in 2011. The investigators discovered that the IP addresses of Freenet users are not hidden. They also saw that there were a lot of child pornography activities, including files and free sites stored in Freenet where child pornography was available. The investigators began collecting the manifest keys of suspected child pornography. After downloading the files, they were able to validate that the files were indeed child pornography.

F. Professor Brian Levine

Brian Levine is a Professor at the University of Massachusetts Amhurst in the College of Information and Computer Sciences. He is also the Director of the University's Cyber

Security Institute. He testified as an expert in networks and network security. Professor Levine has been investigating peer-to-peer networking since approximately 2001. He has also received research grants from the U. S. Government on peer-to-peer networking. He developed an increased interest in network forensics, specifically applying forensically sound techniques to network investigations. He has written several peer reviewed papers on the subject. His most recent paper is on how to do a forensically sound investigation of Freenet.

He has studied how law enforcement uses Freenet to search for child pornography offenders. The basic methodology to find offenders on Freenet is to differentiate between those requesting files and those relaying files. Professor Levine testified that law enforcement uses an algorithm to make that determination. In his research, he validated the mathematical model by creating a simulation of how Freenet works. In analyzing the simulation using the law enforcement algorithm, the false positive rate was roughly two percent.

Professor Levine independently analyzed the data that was presented in the application for the search warrant for Defendant Dickerman’s home. In his analysis, using the data presented in the spreadsheet, he determined that there was a 98 percent probability that Dickerman's IP address was the requester of the file. In addition, Professor Levine verified that based on his analysis, the following information set forth in the affidavit is accurate: “While reviewing requests received by undercover Freenet nodes, located in Missouri, SI Becker observed IP address 172.12.235.62 routing and/or requesting suspected child pornography blocks. The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requestor of the file.” In fact, he stated that his analysis showed that the IP address was more than the “apparent requester,” in fact it shows that there was a very high likelihood that this was the requester. In addition, he agreed that the statement in the affidavit that, "streams of requests for blocks of a particular file from an IP address can be evaluated to determine if the IP address is the likely requester of a file" is true.

G. Stephen Dougherty

In support of his Motion for a *Franks* hearing, Defendant submitted the affidavit of Stephen Dougherty. Dougherty is a software engineer whose qualifications and experience include: earning his Bachelor of Science in Engineering (Computer Science) Magna Cum Laude from the University of Michigan; working as a student contractor for two summers in Google Summer of Code for the Freenet Project; performing open source work for two years in the Freenet community and an additional three as the project's release manager; and skills in relevant programming languages, applications, and operating systems. (Def. Ex. B at 1.)

Dougherty opined that law enforcement's estimation of the probability that received requests *originated* with a peer, as opposed to merely being forwarded through that peer, relies on the assumption that routing is working well, which the law enforcement version of Freenet does not verify. (Def. Ex. B at 2-3.) Without verifying this assumption, Dougherty asserts that there is insufficient information to determine whether a peer is the original requestor of a file, as set forth in the search warrant affidavit. Dougherty contends that a number of factors can cause routing not to work well, "such as when a node has a slower Internet connection than required, or a lossy [sic] internet connection between peers, or a node recently coming online and being joined to peers with those similar problems." *Id.* at 3. He posits that, if other users are having such problems, a law enforcement node may receive more requests for a file by virtue of being "well-equipped [and] high-uptime," rather than because a peer was the original requestor. *Id.* Thus he states that the law enforcement Freenet version does not verify its assumptions.

II. Conclusions of Law and Analysis

A. Motion for *Franks* Hearing

In Defendant's First Motion to Suppress and in his Motion for *Franks* hearing, Defendant argues that the search warrant was issued as a result of false and misleading statements and omissions pertaining to Freenet and the connection to Defendant's IP address. "[W]here the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." *Franks v. Delaware*, 438 U.S. 154, 155–56, 98 S. Ct. 2674, 2676, 57 L. Ed. 2d 667 (1978).

Dickerman argues that (1) the statement in the search warrant affidavit that "The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requestor of the file" was false and misleading and (2) that omitting any discussion of routing issues and the potential for false positives was misleading. In support of his argument, Defendant relies on the affidavit supplied by Stephen Dougherty. Dougherty states that there are a number of reasons that could account for the "number and timing of requests" from this IP address without suggesting that this IP address was the originator.

Defendant has not established that the statement in the affidavit that "The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requestor of the file" was false and misleading. In response to Defendant's motion, the Government provided an Excel spreadsheet showing how SI Becker verified the number and timing of requests. Ex.2. A review of Exhibit 2 establishes that the statement in the affidavit was not false or misleading. In addition, the Government's expert witness Professor Levine testified that in his analysis of the data included in the spreadsheet, there was a 98 percent probability that Dickerman's IP address was the requester of the file. The undersigned finds Professor Levine's testimony credible and therefore, Defendant has not met his burden of showing that the statement was false or misleading.

Defendant's second argument is that the affidavit omitted relevant discussion regarding the behavior of Freenet's routing. "The holding of *Franks v. Delaware* also applies to material that has been deliberately or recklessly omitted from a search-warrant affidavit." *United States v. Butler*, 594 F.3d 955, 961 (8th Cir.2010). However, "[s]uch a finding alone is legally insufficient to justify a *Franks* hearing absent a determination that the intentionally or recklessly omitted information may have rendered the affidavit misleading and may have otherwise made a probable cause finding unsupportable." *United States v. Williams*, 477 F.3d 554, 558 (8th Cir. 2007). To determine probable cause, the issuing judge asks whether, based on the totality of the circumstances set forth in the application, there is a fair probability that contraband or evidence of a crime will be found in a particular place. *Illinois v. Gates*, 462 U.S. 213, 238, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983). Applications "should be examined under a common sense approach and not in a hypertechnical fashion." *United States v. Williams*, 10 F.3d 590, 593 (8th Cir. 1993).

The issue here is whether or not the false positive rate of law enforcement's algorithm was so significant, either generally or in the case at bar, as to defeat probable cause if it had been included in the search warrant application. Professor Levine has studied the algorithm used by law enforcement. He validated the law enforcement algorithm by creating a simulation of how

Freenet works. In his analysis of the simulation, the false positive rate was approximately two percent. In addition, SI Becker testified credibly that he has been involved in 40-50 Freenet investigations and using the algorithm, evidence of child pornography was found on every computer they searched.

In addition, one court has found that where an investigator used a specialized software to search a peer-to-peer file sharing network for child pornography, the use of hash values to identify child pornography on the target computer was sufficient to establish probable cause to search the defendant's residence even though the investigator was unable to download any of the files from the target computer. *United States v. Feldman*, No. 13-CR-155, 2014 WL 7653617, at *8–10 (E.D. Wis. July 7, 2014), *report and recommendation adopted*, No. 13-CR-155, 2015 WL 248006 (E.D. Wis. Jan. 19, 2015).

Defendant also contends that the law enforcement algorithm relies on the faulty assumption that routing between and among the nodes is working well. Defendant's expert Dougherty did not testify at the hearing. However, in an affidavit he asserted that the law enforcement version of Freenet does not verify the assumptions regarding router speed. Professor Levine testified that even if some of the peers had bad connections, it would not change the conclusion that in this case, Dickerman's IP address was the requester of the file.

Here, Defendant has failed to establish that the omitted information regarding router speed and potential false positive results rendered the affidavit misleading or otherwise made a probable cause finding unsupportable. Therefore, it is recommended that Defendant's Motion for a *Franks* hearing be denied.

B. Probable Cause for Search Warrant

a. Judge did not act as rubber stamp

In his First Motion to Suppress Evidence and Statements, as well as in his post hearing briefing, Defendant contends that there was no probable cause for the warrant to search his home. Defendant claims that the judge who issued the search warrant "lacked the technical expertise to determine probable cause based on the contents of the affidavit" and therefore acted as a "rubber stamp for the police." He also claims the search warrant affidavit relied on conclusory statements and failed to give the judge a substantial basis for determining probable cause. Finally, Dickerman argues that the warrant is not entitled to deference under *United States v. Leon*, 468 U.S. 897, 914, 104 S. Ct. 3405, 3416, 82 L. Ed. 2d 677 (1984). He contends that because of the complexity and technical nature of the probable cause determination, the issuing judge's lack of training related to Freenet and computer networks, and the conclusory nature of the statement in the affidavit meant that the judge was not given a substantial basis for determining probable cause and merely rubber stamped law enforcement.

"Reasonable minds frequently may differ on the question whether a particular affidavit establishes probable cause, and therefore the preference for warrants is most appropriately effectuated by according "great deference" to a magistrate's determination. *Spinelli v. United States*, 393 U.S., at 419, 89 S.Ct., at 590. *See Illinois v. Gates*, 462 U.S.at 236, 103 S.Ct., at 2331; *United States v. Ventresca*, 380 U.S. 102, at 108–109, 85 S.Ct. 741, at 745–746.

Deference to the magistrate, however, is not boundless. It is clear, first, that the deference accorded to a magistrate's finding of probable cause does not preclude inquiry into the knowing or reckless falsity of the affidavit on which that determination was based. *Franks v.*

Delaware, 438 U.S. 154, 167, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978). Second, the courts must also insist that the magistrate purport to "perform his 'neutral and detached' function and not serve merely as a rubber stamp for the police." *Aguilar v. Texas*, 378 U.S. 108, 111, 84 S.Ct. 1509, at 1512 (1964). *See Illinois v. Gates*, *supra*, 462 U.S. at 239, 103 S.Ct., at 2332. A magistrate failing to "manifest that neutrality and detachment demanded of a judicial officer when presented with a warrant application" and who acts instead as "an adjunct law enforcement officer" cannot provide valid authorization for an otherwise unconstitutional search. *Lo–Ji Sales, Inc. v. New York*, 442 U.S. 319, 326–327, 99 S.Ct. 2319, 2324–2325, 60 L.Ed.2d 920 (1979); *United States v. Leon*, 468 U.S. 897, 914, 104 S. Ct. 3405, 3416, 82 L. Ed. 2d 677 (1984).

Defendant relies on *United States v. Decker*, 956 F.2d 773 for the proposition that the issuing judge abandoned his neutral and detached role. In *Decker*, a Drug Enforcement Administration ("DEA") agent removed a suspicious package from a UPS processing facility. The package was inspected by a drug sniffing dog which reacted as if the box contained drugs. The officers made a controlled delivery of the package and the recipient was arrested at the door. *See Decker*, 956 F.2d at 774-775. The DEA agent applied for a warrant to search the residence and UPS package. *Id.* The warrant signed by the state court judge was a standard form relating to stolen property, not drugs. While the warrant did specify that the apprehended UPS package was being held by the agent, the issuing judge failed to cross out a standard reference to the UPS package as having been "unlawfully stolen." Moreover, the prosecutor did not sign the warrant, as required by Missouri law. The issuing judge later admitted that these flaws were his fault and acknowledged that the search warrant was not issued in compliance with Missouri law. The judge attributed these oversights to the fact that he was intrigued by the manner in which the agent became suspicious of the package and the ensuing investigation and therefore did not focus on the language of the warrant. *Id.* at 775. More than 300 items were seized during the two day search of the residence. The first item searched was the UPS package which contained over 100 grams of methamphetamine and drug-related documents. Thereafter, the officers seized additional drugs and related paraphernalia located in the Deckers' home. *Id.* at 775–76. After a hearing, the District Court granted Decker's motion to suppress evidence, finding that the issuing judge signed the warrant without reading it and that he failed to note both that the prosecutor had not signed the warrant and that the warrant did not list the property to be seized. Consequently, the district court concluded that the issuing judge acted as a rubber stamp. *Id.* at 777.

The Eighth Circuit Court of Appeals upheld the district court finding that the warrant's glaring omission of the items to be seized supports the district court's finding that the issuing judge never read it. The judge's failure to strike the words "unlawfully stolen" from the warrant further supports this conclusion. The Court of Appeals also stated that the same can be said regarding the judge's failure to ensure that the prosecutor had signed the warrant, as required by Missouri law. Moreover, the judge himself admitted that he issued "the search warrant on the strength of what the officer told me," as opposed to relying on the written warrant and affidavit. *Id.*

Relying on *Decker*, the defendant contends that the issuing judge in this case acted as a rubber stamp. In his post-hearing memorandum, Defendant stated that "the warrant judge 'glazed over the facts' included in the warrant affidavit … and did so because he couldn't understand them." In addition, Defendant points to Judge Borbonus' testimony that the "rest of it might as well have been written in Greek." When asked on direct examination, the Judge agreed that the data underlying the conclusion was Greek to him.

Defendant mischaracterizes some of the Judge's testimony. Judge Borbonus did not testify that he glazed over the facts because he did not understand them. His testimony was, "I would tell you that there was much that I probably glazed over in the sense of what we have just been talking about, but, yes, I read the entire affidavit. I read the entire affidavit." (Tr. 219-220). Furthermore, on cross examination, the judge was asked about the paragraphs in the affidavit that describe how Freenet operates and how law enforcement became aware that Defendant's IP address had requested files of child pornography.

At the hearing Judge Borbonus testified that some of the terminology was Greek to him, however, that does not lead to the conclusion that the judge abandoned his role as a neutral and detached magistrate and acted as a rubber stamp for law enforcement. Unlike the facts of *Decker*, where the warrant referenced stolen property instead of drugs, here the affidavit and search warrant properly referenced the search for child pornography. In *Decker*, the warrant was found to be defective because it did not state the items to be seized and this error was not cured by the details of the affidavit which was not attached to, or incorporated by the warrant. Furthermore, the prosecutor failed to sign the warrant as required by state law and the judge signed a pre-printed form warrant that failed to specify the property to be seized and referred to the UPS package as being "unlawfully stolen." *Decker*, 956 F.2d at 776. In addition, the issuing judge testified that he executed the search warrant on the strength of what the officer told him. *Id.* at 777.

In this case, the warrant did specify the location to be searched and the items to be seized. It also incorporated the information set forth in the affidavit which was attached to the warrant.

Judge Borbonus testified that he did read the affidavit in its entirety and he looked at the warrant to confirm the language matches the address to be searched. In addition, he relied solely on the information in the affidavit and did not get additional information from Detective Slaughter.

Unlike the issuing judge in *Decker*, here, Judge Borbonus acted in a neutral and detached manner and did not act as a rubber stamp for law enforcement.

b. There was a substantial basis for probable cause

Defendant contends that the search warrant affidavit relied on conclusory statements and failed to give the issuing judge a substantial basis for determining probable cause. Specifically, Defendant refers to this statement: "While reviewing requests received by undercover Freenet nodes, located in Missouri, SI Becker observed IP address 172.12.235.62 routing and/or requesting suspected child pornography blocks. The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requestor of the file." Defendant claims that this statement was misleading and false and that the judge's apparent lack of sufficient technical expertise or experience with Freenet compounded the problem.

The Supreme Court observed in *Illinois v. Gates*, that "probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." 462 U.S. at 232. The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him … there is a fair probability that contraband or evidence of a crime will be found in a particular place. *Id*. 462 U.S. 213, 238-39, 103 S.Ct. 2317, 2332.

Defendant argues that the use of the term "significant enough" was conclusory and without factual support in the affidavit. Defendant relies on *United States v. Farlee*, 910 F.Supp.2d 1174, 1185 (D.S.D. 2012). In *Farlee*, the District Court held that there was no probable cause for a search warrant where, "there is nothing in the affidavits for the warrants from which the tribal judge could infer how the tribal police came to identify Farlee as that suspect, other than the terse and conclusory statement that the "investigation revealed." The affidavits contained no information about what investigation occurred to identify a suspect." The Court continued, "These affidavits parallel closely the conclusory statements in cases where the Supreme Court has ruled statements insufficient to support a determination of probable cause." *See Nathanson v. United States*, 290 U.S. 41, 44 (1933) (holding affidavit insufficient to support probable cause when it stated the officer had "cause to suspect and does believe" illegal liquor had been brought by the defendant into United States); *Giordenello v. United States*, 357 U.S. 480, 481, 486, 78 S.Ct. 1245, 2 L.Ed.2d 1503 (1958) (holding that an affidavit that stated that a suspect "did receive, conceal, etc., narcotic drugs ... with knowledge of unlawful importation" was insufficient because, among other reasons, "it does not indicate any sources for the complainant's belief; and it does not set forth any other sufficient basis upon which a finding of probable cause could be made"); *Aguilar*, 378 U.S. at 115–16, 84 S.Ct. 1509 (holding affidavit insufficient to support a probable cause determination when it stated that "[a]ffiants have received reliable information from a credible person and do believe" heroin to be in the suspect's home). *Id*.

The undersigned finds the analysis in *Farlee* and its supporting case law instructive. In all of those cases, the courts found there was no substantial basis for a probable cause finding because there were no facts underlying the conclusion set forth in the affidavits. In this case, the affidavit clearly sets forth the basis of the investigative techniques used to determine whether Defendant's IP address was the requester of the files containing child pornography. Furthermore, the testimony at the evidentiary hearing established the reliability of the method used by law enforcement to determine whether a Freenet peer is a requester or relayer of a file.

Search warrants, once issued are presumed to be validly issued. *Franks*, 438 U.S. at 171. The Eighth Circuit Court of Appeals assesses probable cause from the viewpoint of a reasonably prudent police officer acting in the circumstances of the particular case." *United States v. Seidel*, 677 F.3d 334, 337 (8th Cir. 2012) (per curiam) (quoting *United States v. Reinholz*, 245 F.3d 765, 776 (8th Cir. 2001)). "A supporting affidavit establishes probable cause to issue a search warrant if it 'sets forth sufficient facts to establish that there is a fair probability that contraband or evidence of criminal activity will be found in the particular place to be searched.'" *Brackett*, 846 F.3d at 992 (quoting *United States v. Snyder*, 511 F.3d 813, 817 (8th Cir. 2008)). "The determination of whether or not probable cause exists to issue a search warrant is to be based upon a common-sense reading of the entire affidavit." *Seidel*, 677 F.3d at 338 (quoting *United States v. Sumpter*, 669 F.2d 1215, 1218 (8th Cir. 1982)); *United States v. Davis*, 867 F.3d 1021, 1027 (8th Cir. 2017). In this case, the affidavit before Judge Borbonus set forth sufficient facts to establish that there was a fair probability that evidence of child pornography would be found on the computer associated with Defendant Dickerman's IP address.

c. *Leon* Exception

Even if the affidavit had not been sufficient to establish probable cause, law enforcement officers relied in good faith on the probable cause determination by the issuing state court judge when executing the warrant and searching Dickerman's residence. *See United States v. Leon*, 486 U.S. 897, 922 (1984). "Under the *Leon* good-faith exception, disputed evidence will be admitted if it was objectively reasonable for the officer executing a search warrant to have relied in good faith on the judge's determination that there was a probable cause to issue the warrant." *Grant*, 490 F.3d at 632. Although Defendant argues that the *Leon* good faith exception cannot be applied in cases involving a *Franks* violation, that argument is without merit because the undersigned finds that there was no *Franks* violation. Accordingly, even if the warrant affidavit had been insufficient to establish probable cause, the disputed evidence is still admissible because the officers executing the warrant acted in good faith. *See id.*

C. Supplemental Motion to Suppress

a. Third Party Expectation of Privacy

Defendant additionally argues that SI Becker's use of the law enforcement version of Freenet to capture data and content not observable by the typical Freenet user and analyze it in a way that would be impossible for the typical user, constituted a warrantless search and seizure. Defendant argues that, as with the contents of emails, he had a reasonable expectation of privacy in the electronic communications both originating and forwarded from his computer using Freenet and emphasizes that, in using Freenet, he went to greater lengths to protect his privacy than an email user.

In *Katz*, the Supreme Court extended Fourth Amendment protection beyond the common-law trespassory test, holding that a recording device attached to the outside of a public telephone booth was a warrantless search despite the lack of physical intrusion. *Katz v. United States*, 389 U.S. 347, 353, 88 S. Ct. 507, 512, 19 L. Ed. 2d 576 (1967). "[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test." *United States v. Jones*, 565 U.S. 400, 409, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012). The *Katz* test requires: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" 389 U.S. at 361 (Harlan, J., concurring). Under *Katz*, "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." 389 U.S. at 351. However, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Id.*

The third party doctrine, formulated prior to *Katz*, provides that information voluntarily disclosed to a third party, including an undercover government agent, is not protected by the Fourth Amendment. In *Hoffa v. United States*, the Supreme Court held that the Fourth Amendment does not protect an individual who unknowingly converses with a government agent, reasoning that the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." 385 U.S. 293, 302, 87 S. Ct. 408, 413, 17 L. Ed. 2d 374 (1966); *see also Katz*, 389 U.S. at 363 n.** (White, J., concurring) ("The Fourth Amendment does not protect against unreliable (or law-abiding) associates."). Similarly, in *On Lee v. United States* and *Lopez v. United States*, the Court approved the transmission and recording of conversations with government agents. 343 U.S. 747, 72 S. Ct. 967, 96 L. Ed. 1270 (1952); 373 U.S. 427, 83 S. Ct. 1381, 10 L. Ed. 2d 462 (1963); *see also Katz*, 389 U.S. at 363 n.** (White, J., concurring) ("It is but a logical and reasonable extension of this principle that a man take the risk that his hearer, free to memorize what he hears for later verbatim repetitions, is instead recording it or transmitting it to another.").

Post-*Katz*, in *United States v. White*, the Court again approved the transmission and recording of conversations with undercover government agents and affirmed that *Hoffa* and *Lopez* were still good law: "If the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case." 401 U.S. 745, 752, 91 S. Ct. 1122, 1126, 28 L. Ed. 2d 453 (1971).

In *United States v. Miller*, the Supreme Court extended the third party doctrine to cover bank records, reasoning that "This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." 25 U.S. 435, 443, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976). In *Smith v. Maryland*, the Court extended the third party doctrine to cover dialed phone numbers. 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979).

The third party doctrine has been frequently criticized in the context of emerging technology and government surveillance thereof. Indeed, Congress enacted the Electronic Communications Privacy Act and the Stored Communications Act in large part to remedy the lack of Fourth Amendment protection under the third party doctrine. Justice Sotomayor has called for reconsideration of the doctrine:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g., Smith*, 442 U.S., at 742, 99 S.Ct. 2577; *United States v. Miller*, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice ALITO notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," *post*, *418 at 962,

> and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. See *Smith,* 442 U.S., at 749, 99 S.Ct. 2577 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); see also *Katz,* 389 U.S., at 351–352, 88 S.Ct. 507 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

Jones, 565 U.S. at 417–18 (Sotomayor, J., concurring). In line with Justice Sotomayor's view, the Sixth Circuit previously held that users have a reasonable expectation of privacy in the contents of their emails and that an Internet Service Provider is merely an intermediary. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

Dickerman relies on *Kyllo v. United States*, *United States v. Jones*, and *Florida v. Jardines* for support. However, all three Supreme Court opinions authored by the late Justice Scalia rely on trespassory principles or the sanctity of the home. In *Kyllo*, the Court held that law enforcement's use of thermal imaging technology was a warrantless search, reasoning that "[w]here, as here, the Government uses a device that is not in general public use, to explore the details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Kyllo v. United States*, 533 U.S. 27, 40, 121 S. Ct. 2038, 2046, 150 L. Ed. 2d 94 (2001). In *Jones*, the Court held that the installation and use of a GPS device on a vehicle was a warrantless search because the government physically occupied the defendant's "effects" for the purpose of obtaining information. *United States v. Jones*, 565 U.S. 400, 404–06, 132 S. Ct. 945, 949–50, 181 L. Ed. 2d 911 (2012). Finally, in *Jardines*, the Court held that the use of a drug-sniffing dog on a homeowner's porch was a warrantless search because the government physically entered and occupied the "curtilage" of the house to gather information. *Florida v. Jardines*, 133 S. Ct. 1409, 1414, 185 L. Ed. 2d 495 (2013).

As the Government notes, federal courts are in agreement that an individual does not have a reasonable expectation of privacy in files he makes available for download on a conventional peer-to-peer file sharing network. *See United States v. Stults*, 575 F.3d 834, 842–43 (8th Cir. 2009); Susan W. Brenner, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, 81 Miss. L.J. 1229, 1241–42 (2012). The Eighth Circuit has reasoned:

> We hold that Stults had no reasonable expectation of privacy in files that the FBI retrieved from his personal computer where Stults admittedly installed and used LimeWire to make his files accessible to others for file sharing. One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking. As a result, "[a]lthough as a general matter an individual has an objectively reasonable expectation of privacy in his personal computer, we fail to see how this expectation can survive [Stults's] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program." *Ganoe*, 538 F.3d at 1127 (internal citation omitted). Even if we assumed that Stults "did not know that others would be able to access files stored on his own computer," Stults did know that "he had file-sharing software on his computer; indeed, he admitted that he used it—he says to get music [and to download pornography]." *Id.* As a result, Stults "opened up his download folder to the world, including Agent [Cecchini]." *Id.* "Having failed to demonstrate an expectation of privacy that society is

> prepared to accept as reasonable, [Stults] cannot invoke the protections of the Fourth Amendment." *Id.*

Stults, 575 F.3d at 842. This line of cases is distinguishable from the instant case in two respects: (1) the alleged warrantless search or seizure in this case was the government's logging and analysis of requests for blocks that, based on their hash value (block key), were known to be blocks from a child pornography file, and (2) unlike conventional peer-to-peer file sharing networks, Freenet was designed with the express purpose of protecting user anonymity.

The first distinction makes the case for exemption even stronger here. Here, law enforcement used the peer-to-peer network to log requests received by its computer rather than using it to retrieve files from another computer. It seems that an individual has less of a privacy interest in requests sent to another computer than in files stored on his computer.

The Government argues persuasively that this case is substantially analogous to the origins of the third party doctrine, namely, that an otherwise voluntary exchange with undercover government agents and the recording thereof is not protected by the Fourth Amendment. Freenet is intended to protect anonymity, however that leads to anonymous association. Dickerman knowingly downloaded an application that networked his computer with those of complete strangers for the purpose of sharing files. In doing so, he assumed the risk that one of his associates would be less than trustworthy. *See United States v. Matish*, 193 F. Supp. 3d 585, 615 (E.D. Va. 2016) (finding no reasonable expectation of privacy in IP address despite subjective expectation of privacy based on anonymity purpose of Tor network). While the First Amendment may provide some protection for associational privacy, the Fourth Amendment does not. *See Katz*, 389 U.S. at 350 (discussing distinction between Fourth Amendment and First Amendment protection of privacy).

b. Electronic Communication Privacy Act

Finally, Defendant argues that the logging of information related to the block requests by the law enforcement's use of Freenet violates the Electronic Communication Privacy Act (ECPA). "The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically." *Electronic Communications Privacy Act of 1986 (ECPA) 18 U.S.C. § 2510-22* https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

The procedure for interception of wire, oral, or electronic communications is set forth in 18 U.S.C.A. § 2518. "Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application." 18 U.S.C.A. § 2518.

Defendant contends that when the law enforcement version of Freenet logged the IP address, key, and date and time of requests, that constituted an interception of electronic communications under 18 U.S.C. § 2510. In addition, he claims that SI Becker acquired the content of communications and used that content to match the hash values of known child pornography files, and stored the data that he intercepted. Defendant correctly notes that SI Becker did not apply for authorization to capture such information. Defendant also argues that the logging of information by the law enforcement node violated reasonable expectations of privacy under the Act. The Government argues that authorization is unnecessary because the information logged by the law enforcement node does not constitute an interception of the content of electronic communications as proscribed by the ECPA. 18 U.S.C. § 2510(4).

Under the ECPA, "intercept means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." The "content" of electronic communications includes any information concerning the substance, purport, or meaning of the communication. 18 U.S.C.A. § 2510(8). And "electronic communication means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."

Here, the law enforcement node logs the IP address; date; time; and key (hash value of the file) when it receives a request for a file. Under the definitions, it is clear that law enforcement is capturing electronic communication from the node requesting a file. However, it does not appear that the information being logged by the law enforcement node is "content" under the ECPA. The data collected by law enforcement does not include information concerning the substance, purport or meaning of the communication.

Even if the information logged by law enforcement is deemed to be content, there is no violation of the ECPA because the law enforcement node was a party to the communication. Title I of the Electronic Communications Privacy Act of 1986 provides that it is not unlawful to intercept such a communication if a party to the communication has given prior consent to the interception. Nor does such an interception violate the Fourth Amendment." *Id.* (citing *United States v. White*, 401 U.S. 745, 753 (1971); 18 U.S.C. § 2511(2)(c)). "The government bears the burden of proving consent." *Id.* "Consent may be express or implied, but in either case, there must be actual consent." *Id.* (citing *Deal v. Spears*, 980 F.2d 1153, 1157 (8th Cir.1992)). Here the Government has carried its burden of proving consent. Defendant Dickerman's computer requested the file from its peers, including the law enforcement node. The law enforcement node reviewed the request for that block of file to relay to Defendant's computer. That communication between the nodes makes the computers parties to the communication. Therefore, the ECPA was not violated.

Furthermore, even if this court were to find a violation of the ECPA, exclusion of the evidence is not an appropriate remedy. The suppression provision in the Act provides no basis for moving to suppress electronic communications. By its terms, 18 U.S.C. § 2515 applies *only* to "wire or oral communication[s]," and not to "electronic communications":

> Whenever any *wire or oral communication* has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

18 U.S.C. § 2515. Despite the fact that the ECPA amended numerous sections of the Wiretap Act to include "electronic communications," the ECPA did not amend § 2515. *United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003).

In *United States v. Meriwether,* the Sixth Circuit held that it could not "under the ECPA grant appellant's requested remedy—suppression [because t]he ECPA does not provide an independent statutory remedy of suppression for interceptions of electronic communications." 917 F.2d 955, 960 (6th Cir.1990) (citations omitted); *see also, e.g., United States v. Reyes,* 922 F.Supp. 818, 837 (S.D.N.Y.1996) (holding that exclusion of evidence is not a remedy for the ECPA violation).

CONCLUSION AND RECOMMENDATIONS

Accordingly**,**

IT IS HEREBY RECOMMENDED that First Motion to Suppress Evidence and Statements [Doc. #20] should be **DENIED**;

IT IS FURTHER RECOMMENDED that Defendant's First Motion for *Franks* Hearing [Doc. #21] should be **DENIED**; and

IT IS FINALLY RECOMMENDED that Defendant's Supplemental Motion to Suppress Evidence [Doc. #33] should be **DENIED**.

The parties are advised that they have fourteen (14) days in which to file written objections to this report and recommendation pursuant to 28 U.S.C. § 636(b)(1). Failure to timely file objections may result in a waiver of the right to appeal questions of fact.

Dated this 26th day of September, 2017.

/s/ Nannette A. Baker
NANNETTE A. BAKER
UNITED STATES MAGISTRATE JUDGE